Ruijie Reyee RG-ES Series Switches

ESW_1.0(1)B1P24

Web-based Configuration Guide

Document Version: V1.0
Date: 2023.11.20

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

❗ **Warning**

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

⚠ **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

ℹ **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

✓ **Specification**

An alert that contains a description of product or version support.

3. Note

This manual introduces the product model, port type and GUI for your reference. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

1 Login

1.1 Configuration Environment Requirements

- Browser: Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/IE kernel-based browsers are supported. Exceptions such as messy code and format errors may occur when other browsers are used.
- Resolution: 1024 x 768 or a higher resolution is recommended. Exceptions such as font alignment error and format error may occur when other resolutions are used.

1.2 Login to the Web Management System

1.2.1 Connecting the Device

Connect the switch port with the network port of the PC through an Ethernet cable. Configure the PC with an IP address in the same network segment as the default IP address of the switch so that the PC can ping the switch. For example, set the IP address of the PC to 10.44.77.100.

Table 1-1 Default Configuration

Feature	Default Setting
Device IP Address	10.44.77.200
Password	A username is not required when you log in for the first time. The default password is admin.

You can use the default password “admin” to log in to the switch for the first time. To ensure security, you are advised to change the password after login, and update the password regularly.

After five failed attempts, you must wait one minute before re-entering the password to login.

1.2.2 Login to the Web Management System

(1) Enter the IP address (10.44.77.200 by default) of the device into the address bar of the browser to access the login page.

Note

If the static IP address of the device is changed, or the device dynamically obtains a new IP address, the new IP address can be used to access the web management system of the device as long as the PC and the device are in the same network segment of a LAN.

(2) Enter the username and password (default username/password: admin/admin), and then click **Log In** to enter the homepage of the web management system.

Users will be prompted to reset the default password upon their first login to the web management system. If the password is the default password, users are not allowed to configure the device. They need to log in to the web management system with the reset password to configure and manage the device. For details about password settings, see Chapter 6.2.

If you forget the device IP address or password, press and hold the **Reset** button on the device panel for more than 5 seconds to restore factory settings. After restoration, you can use the default IP address and password to log in.

⚠ **Caution**

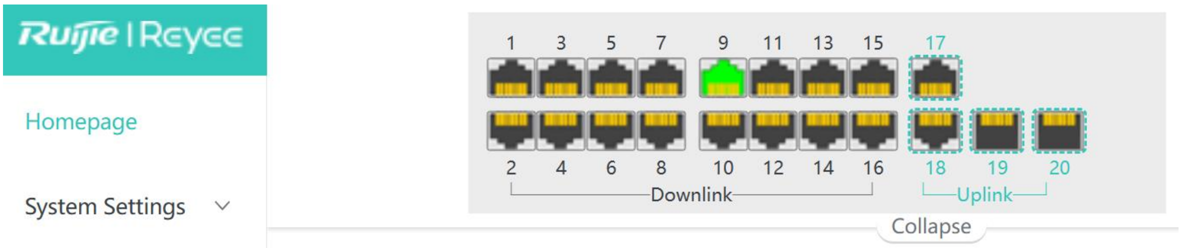
Restoring factory settings will delete the current configurations. Exercise caution when performing this operation.

2 Port Settings

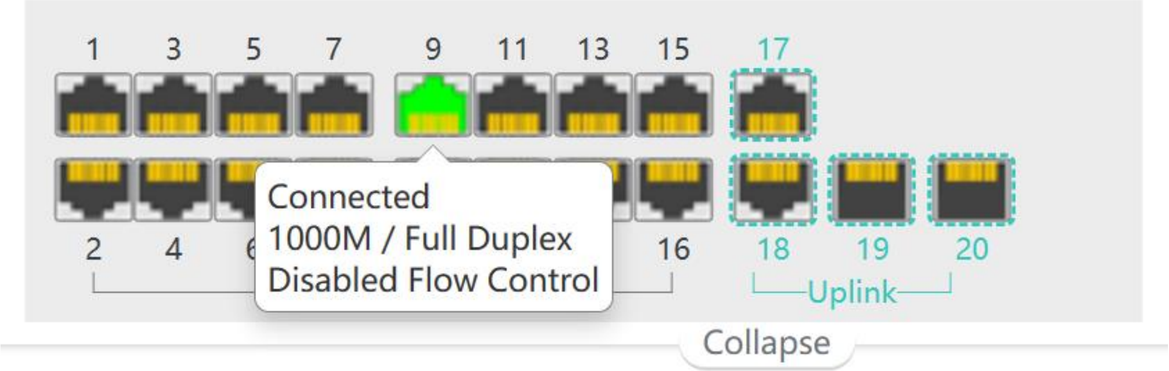
2.1 Managing Port Information

2.1.1 Port Status Bar

The port status bar is at the top of the web page, showing port ID, port attribute (uplink/downlink), and the connection status. Click **Collapse** to hide the port status bar.

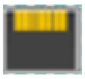
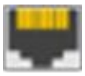
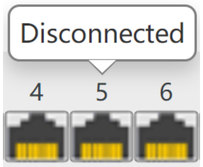


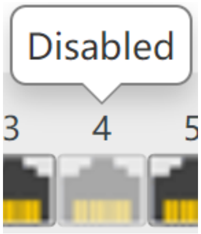
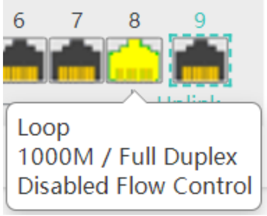
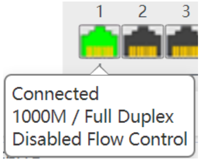
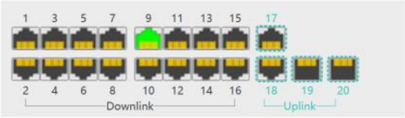
Different colors and shapes of the port icons represent different port statuses. See Table 2-1 for details. Move the cursor over a port icon and the port status will be displayed, including the connection status, port rate, duplex mode, and flow control status.



Connected
1000M / Full Duplex
Disabled Flow Control

Table 2-1 Port Icons

Port Icon	Description
	The port icon is in the shape of a square, showing the port is a fiber port.
	The port icon is in the shape of an RJ-45 connector, showing the port is a copper port.
	The color of the port icon is black, showing the port is disconnected.

 Disabled 	The color of the port icon is gray, showing the port is disabled and cannot receive or transmit packets.
 Loop 1000M / Full Duplex Disabled Flow Control	The color of the port icon is yellow, showing there is a loop.
 Connected 1000M / Full Duplex Disabled Flow Control	The color of the port icon is green, showing the port is working normally.
 	The number above the port icon is the port ID used to identify the device port. With the port ID, users can specify the port they want to configure.
 1 3 5 7 9 11 13 15 17 2 4 6 8 10 12 14 16 18 19 20 Downlink Uplink	The device port is classified into the uplink port and the downlink port. The uplink port is used to connect network devices in the upper layer and access the core network. The downlink port is used to connect the endpoints. When port isolation is enabled, the downlink ports of the device are isolated from each another, and they can only communicate with the uplink ports. For details, see Chapter 2.4.

2.1.2 Port Info Overview

Choose **Homepage**.

The homepage displays the global port information, including the port status, the packet receiving/transmission rate (Rx/Tx rate), port isolation status and loop detection status. Besides, it supports searching for the downlink device.

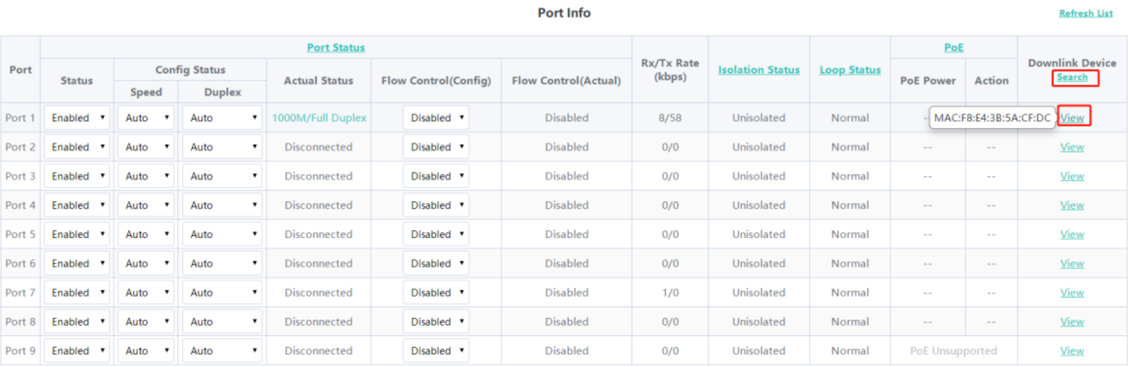
Click **Port Status** to configure the basic port attributes. For details, see Chapter 2.2.

Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see Chapter 2.4.

Click **Loop Status** to enable loop guard function. After a loop occurs, the port causing the loop will be shut down automatically. For details, see 4.3.

Click **Search** in the **Downlink Device** column to search for the downlink device of the selected port. After the search is done, click **View** to view the MAC address of the downlink device.

Click **Refresh List** to fetch the latest port information.



Port Info

Refresh List

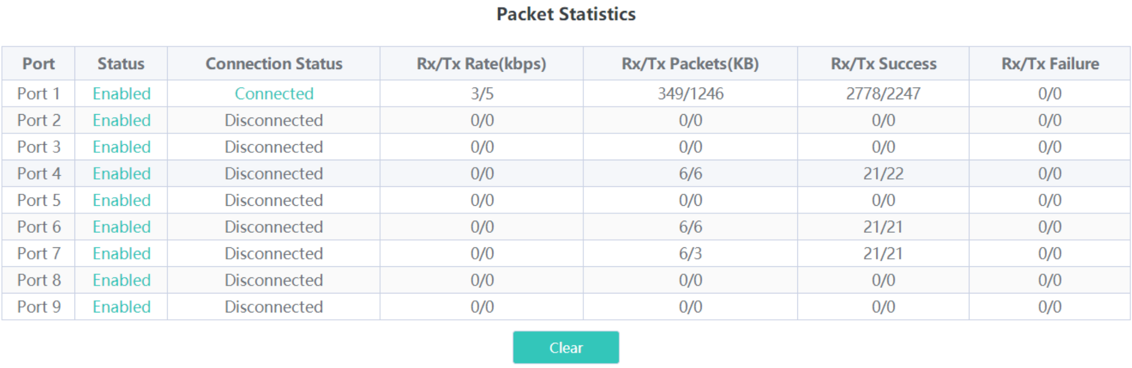
Port	Port Status						Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)				PoE Power	Action	Search
		Speed	Duplex									
Port 1	Enabled ▾	Auto ▾	Auto ▾	1000M/Full Duplex	Disabled ▾	Disabled	8/58	Unisolated	Normal	-	MAC:F8:E4:3B:5A:CF:DC	View
Port 2	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 3	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 4	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 5	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 6	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 7	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	1/0	Unisolated	Normal	--	--	View
Port 8	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	--	--	View
Port 9	Enabled ▾	Auto ▾	Auto ▾	Disconnected	Disabled ▾	Disabled	0/0	Unisolated	Normal	PoE Unsupported		View

2.1.3 Port Packet Statistics

Choose **Monitoring** > **Packet Statistics**.

The **Packet Statistics** page displays the port status, the connection status, Rx/Tx rate (kbps), Rx/Tx packets (KB), Rx/Tx success, and Rx/Tx failure.

Click **Clear** to clear current packet statistics of all ports and reset the statistics.



Packet Statistics

Port	Status	Connection Status	Rx/Tx Rate(kbps)	Rx/Tx Packets(KB)	Rx/Tx Success	Rx/Tx Failure
Port 1	Enabled	Connected	3/5	349/1246	2778/2247	0/0
Port 2	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 3	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 4	Enabled	Disconnected	0/0	6/6	21/22	0/0
Port 5	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 6	Enabled	Disconnected	0/0	6/6	21/21	0/0
Port 7	Enabled	Disconnected	0/0	6/3	21/21	0/0
Port 8	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 9	Enabled	Disconnected	0/0	0/0	0/0	0/0

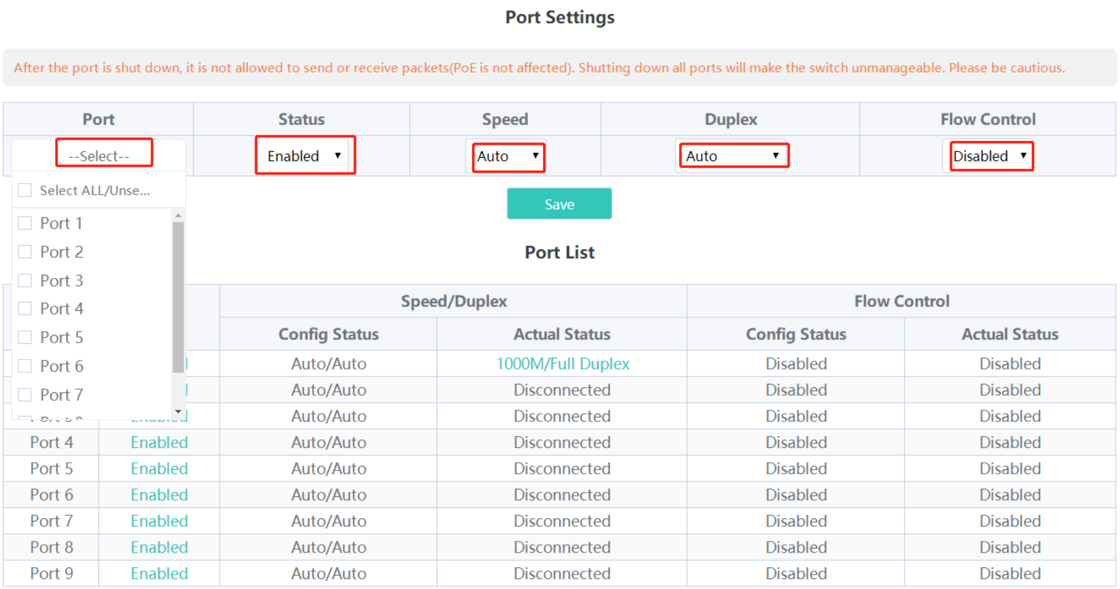
2.2 Setting and Viewing Port Attributes

Choose **Switch Settings** > **Port Settings**.

2.2.1 Port Settings

Users can set the basic attributes of the Ethernet ports in batches.

Click **Select** in the **Port** column to display options of all device ports. Select the ports you want to configure, and then select the port status, port rate, port duplex mode, flow control status, and click **Save**.



Port Settings

After the port is shut down, it is not allowed to send or receive packets(PoE is not affected). Shutting down all ports will make the switch unmanageable. Please be cautious.

Port	Status	Speed	Duplex	Flow Control
--Select--	Enabled ▾	Auto ▾	Auto ▾	Disabled ▾

□ Select ALL/Unse...
□ Port 1
□ Port 2
□ Port 3
□ Port 4
□ Port 5
□ Port 6
□ Port 7

Save

Port List

		Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
		Auto/Auto	1000M/Full Duplex	Disabled	Disabled
		Auto/Auto	Disconnected	Disabled	Disabled
		Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

Table 2-2 Basic Port Configuration Parameters

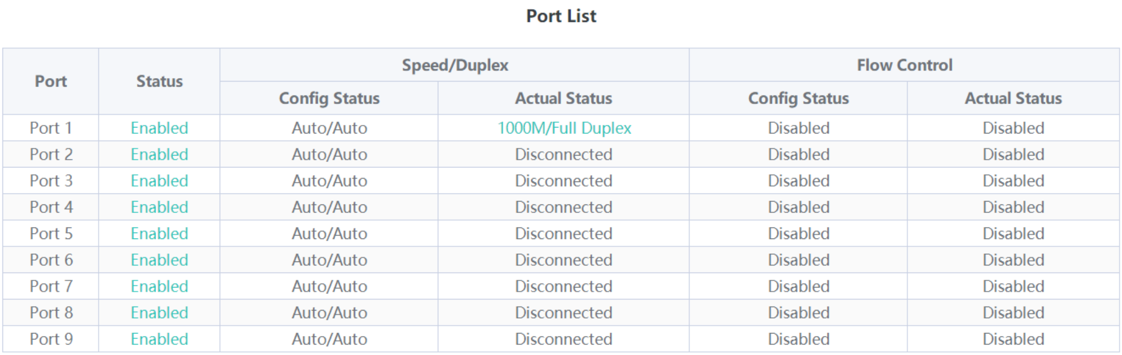
Parameter	Description	Default
Port	Select the ports you want to configure.	NA
Status	When the port is disabled, it cannot receive or transmit packets (PoE is not affected).	Enabled
Speed	Configure the operating speed of the Ethernet physical port. When the speed is set to **Auto**, it means that it is determined by the auto-negotiation between the local port and the peer port. The negotiated speed can be any speed within the port capability.	Auto
Duplex	● Full duplex: The port can receive packets while sending packets. ● Half duplex: The port can receive or send packets at a time. ● Auto-negotiation: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port.	Auto
Flow Control	After enabling the flow control feature, the port will process the received flow control frames and send flow control frames when flow congestion occurs.	Disabled

⚠ **Caution**

Shutting down all ports will make the switch unmanageable. Exercise caution when performing this operation.

2.2.2 Port Status

Users can view the configuration status of the port attributes and check whether these configurations are active, including the port rate, duplex mode, and flow control status.



Port List

Port	Status	Speed/Duplex		Flow Control	
		Config Status	Actual Status	Config Status	Actual Status
Port 1	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
Port 2	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 3	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled

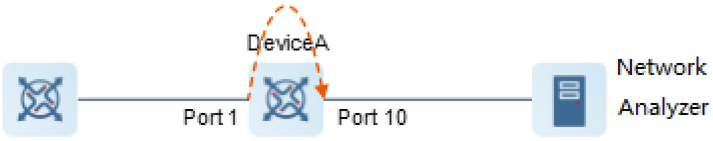
2.3 Port Mirroring

2.3.1 Overview

In network monitoring and troubleshooting scenarios, users need to analyze data traffic on suspicious network nodes or device ports. When port mirroring is enabled, packets received and transmitted on the source port will be mirrored to the mirror port (destination port). Users can monitor and analyze the packets on the mirror port through network analyzer without affecting the normal data forwarding of the monitored device.

As Figure 2-1 shows, by configuring port mirroring on Device A, the packets on Port 1 are mirrored to Port 10. Though the network analyzer is not directly connected to Port 1, it can receive all packets on Port 1 and is able to monitor the data traffic on Port 1.

Figure 2-1 Operating Principle of Port Mirroring



2.3.2 Configuration Steps

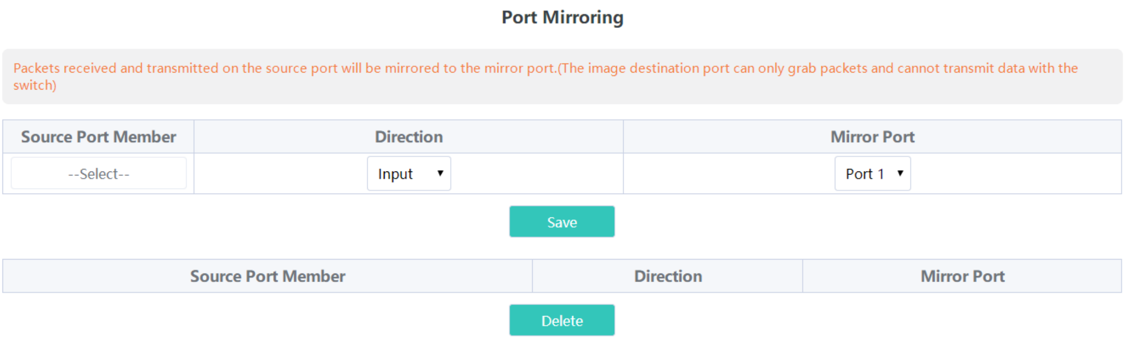
Choose **Switch Settings** > **Port Mirroring**.

Select the source port, the monitoring direction, and the mirror port, and click **Save**. The device supports configuring one port mirroring rule.

If you want to delete port mirroring configuration, click **Delete**.

Caution

- You can select multiple source ports but only one mirror port. The source ports cannot contain the mirror port.



Port Mirroring

Packets received and transmitted on the source port will be mirrored to the mirror port.(The image destination port can only grab packets and cannot transmit data with the switch)

Source Port Member	Direction	Mirror Port
--Select--	Input	Port 1

Source Port Member	Direction	Mirror Port

Table 2-3 **Port Mirroring Parameters**

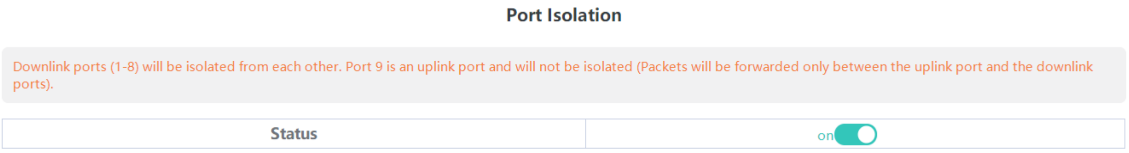
Parameter	Description
Source Port Member	The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. Users can select multiple source ports. Packets on these ports will be mirrored to one mirror port.
Direction	Direction of the data traffic monitored on the source port: ● Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. ● Input: The packets received by the source port will be mirrored to the mirror port. ● Output: The packets transmitted from the sourced port will be mirrored to the mirror port.
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and it transmits packets on the source port to the monitoring device.

2.4 Port Isolation

Choose **Switch Settings** > **Port Isolation**.

Port isolation is used for isolating layer-2 packets. When port isolation is enabled, the downlink ports are isolated from each other but can communicate with uplink ports.

Port isolation is disabled by default. Toggle the switch to **On** to enable port isolation.



Port Isolation

Downlink ports (1-8) will be isolated from each other. Port 9 is an uplink port and will not be isolated (Packets will be forwarded only between the uplink port and the downlink ports).

Status	on

Caution

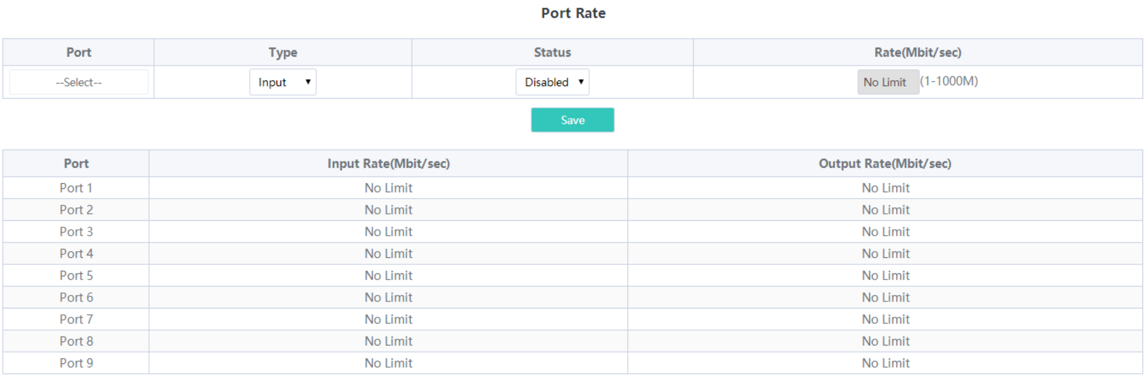
The number of the uplink/downlink ports and port IDs of different devices vary. Please refer to the actual information of the device.

2.5 Port-based Rate Limiting

Choose **QoS Settings** > **Port Rate**.

Users can configure rate limiting rules for packets in the input direction and the output direction of ports. There is no rate limiting on ports by default.

Select the port you want to configure, then select the rate limiting type and status, and enter the rate limit. Click **Save** to save the configuration. The configuration will be displayed accordingly in the **Port Rate** table right below the **Save** button.



Port Rate

Port	Type	Status	Rate(Mbit/sec)
--Select--	Input ▾	Disabled ▾	No Limit (1-1000M)

Port	Input Rate(Mbit/sec)	Output Rate(Mbit/sec)
Port 1	No Limit	No Limit
Port 2	No Limit	No Limit
Port 3	No Limit	No Limit
Port 4	No Limit	No Limit
Port 5	No Limit	No Limit
Port 6	No Limit	No Limit
Port 7	No Limit	No Limit
Port 8	No Limit	No Limit
Port 9	No Limit	No Limit

Table 2-4 **Rate Limiting Parameters**

Parameter	Description	Default
Port	Users can select multiple ports for rate limiting configuration in batches.	NA
Type	The direction of the rate-limited data traffic: ● Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets. ● Input: Rate limiting for packets received by the port. ● Output: Rate limiting for packets transmitted from the port.	NA
Status	Users can decide whether to enable or disable rate limiting.	Disabled
Rate (Mbit/sec)	The maximum rate at which packets are forwarded over the port.	No limit

Note

- The rate limiting range for RG-ES220GC-P, RG-ES228GC-P switches ports is from 1 to 1000M.

2.6 Management IP Address

Choose **System Settings** > **IP Settings**.

Users can configure the management IP address of the device. By accessing the management IP address, users can configure and manage the device.

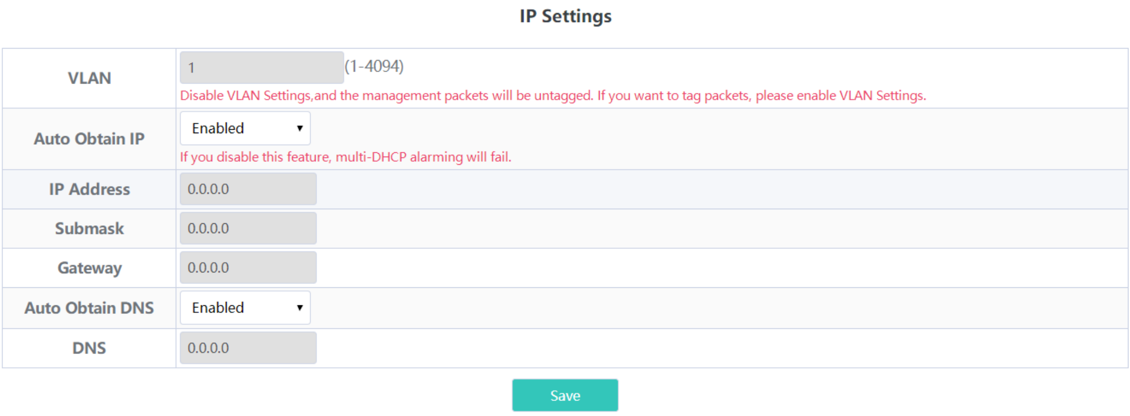
There are two Internet types available:

- Dynamic IP address: Enable **Auto Obtain IP** feature to use the IP address assigned dynamically by the uplink DHCP server.
- Static IP address: Disable **Auto Obtain IP** feature to use the fixed IP address configured manually by the user.

Enable **Auto Obtain IP** feature, and the device will automatically obtain various parameters from the DHCP server. Users can select whether to obtain a DNS address automatically from the DHCP server. If **Auto Obtain DNS** feature is disabled, users need to configure a DNS address manually.

After disabling **Auto Obtain IP** feature, users need to manually configure the IP address, subnet mask, gateway IP address, and DNS address. Click **Save** to enforce the configuration.

VLAN is used for managing VLAN tag of the management packets. Disable VLAN settings, and the management packets will be untagged, and management VLAN configuration is not supported. The management VLAN of the device is VLAN 1 by default.



IP Settings

VLAN	1 (1-4094) Disable VLAN Settings,and the management packets will be untagged. If you want to tag packets, please enable VLAN Settings.
Auto Obtain IP	Enabled If you disable this feature, multi-DHCP alarming will fail.
IP Address	0.0.0.0
Submask	0.0.0.0
Gateway	0.0.0.0
Auto Obtain DNS	Enabled
DNS	0.0.0.0

Note

- Disable VLAN settings, and the management packets will be untagged. If you want to tag packets, please enable VLAN settings. For details, see Chapter 3.2.1.
- The management VLAN must be selected from the existing VLANs. To create a static VLAN, refer to Chapter 3.2.2.
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web management system. For details, see Chapter 3.2.3.
- If you disable **Auto Obtain IP** feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see Chapter 7.2.

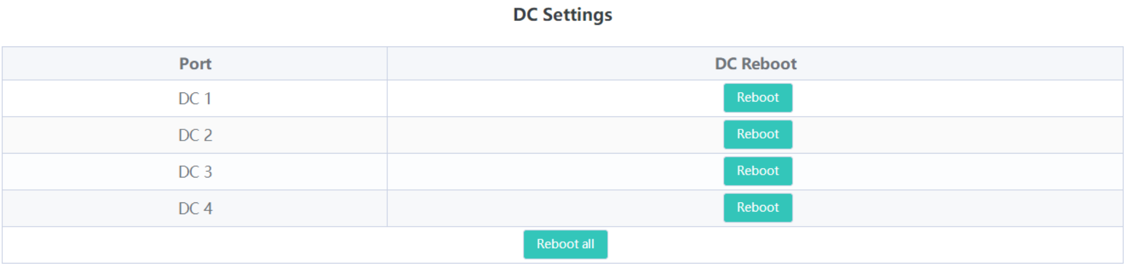
2.7 DC Port Reboot

⚠ **Caution**

Only RG-FS306-D switch supports this feature.

Choose **DC Settings**.

Select the DC port you want to reboot, and click **Reboot** to reboot the selected DC port. Click **Reboot all** to reboot all DC ports of the device.



DC Settings

Port	DC Reboot
DC 1	Reboot
DC 2	Reboot
DC 3	Reboot
DC 4	Reboot

3 Switch Settings

3.1 Managing MAC Address

3.1.1 Overview

The MAC address table records mappings of MAC addresses and ports to VLANs.

The device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC address in the packet, the device forwards the packet through the port specified by the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all ports other than the receiving port in broadcast mode.

MAC address entries are classified into the following types:

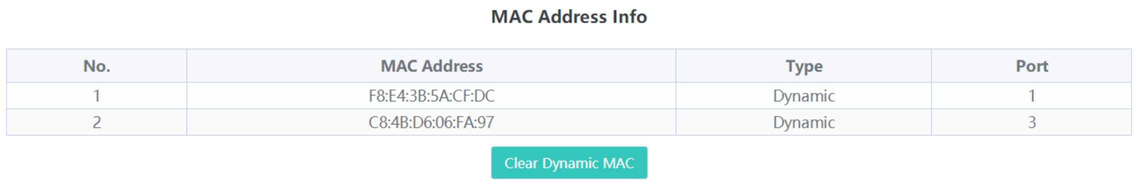
- Static MAC address entries: Static MAC address entries are manually configured by the users. Packets whose destination MAC address matches the one in such an entry are forwarded through the corresponding port.
- Dynamic MAC address entries: Dynamic MAC address entries are learned dynamically by the device. They are generated automatically by the device.

3.1.2 Viewing MAC Address Table

Choose **Switch Settings** > **MAC Address Info**.

This page displays the MAC address of the device, including the static MAC address configured manually by the users and the dynamic MAC address learned automatically by the device.

Click **Clear Dynamic MAC** to clear the dynamic MAC address learned by the device. The device will re-learn the MAC address and generate a MAC address table.



MAC Address Info

No.	MAC Address	Type	Port
1	F8:E4:3B:5A:CF:DC	Dynamic	1
2	C8:4B:D6:06:FA:97	Dynamic	3

Note

- If you disable VLAN, the device will forward packets according to only the destination MAC address. VLAN ID is not displayed in the MAC address table.
- Up to 100 MAC addresses are displayed.

3.1.3 Searching for MAC Address

Choose **Switch Settings** > **Search MAC**.

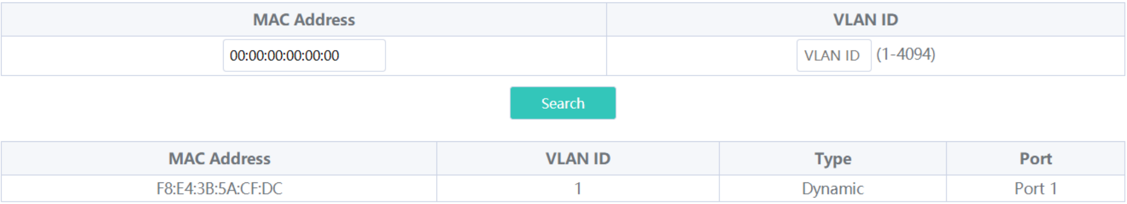
Users can search for MAC address entries according to MAC address and VLAN ID.

⚠ **Caution**

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table.MAC address entries can only be found through MAC address.

Enter MAC address and VLAN ID, and then click **Search**. The MAC address entries that meet the search criteria will be displayed in table right below the **Search** button. Moreover, users can enter partial characters of the MAC address for fuzzy search.

MAC Address Search



MAC Address	VLAN ID
00:00:00:00:00:00	VLAN ID (1-4094)

MAC Address	VLAN ID	Type	Port
F8:E4:3B:5A:CF:DC	1	Dynamic	Port 1

3.1.4 Configuring Static MAC Address

Choose **Switch Settings** > **Static MAC**.

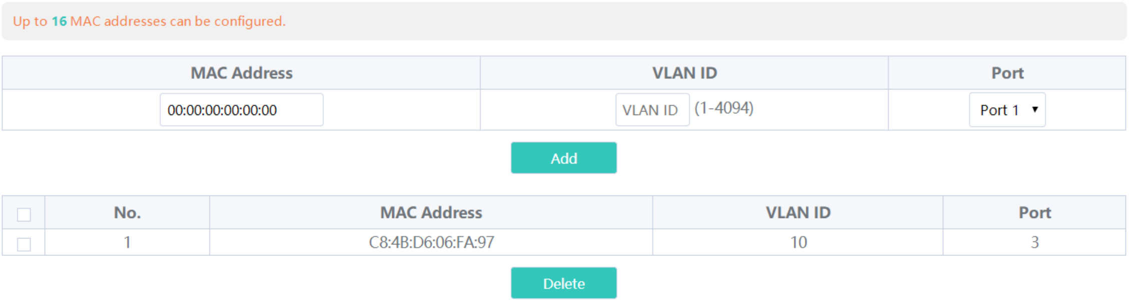
By configuring a static MAC address, users can manually bind the MAC address of a downlink network device with a port of the switch. After you add a static MAC address, when the device receives a packet destined to this address from VLAN, it forwards the packet to the specified port.

⚠ **Caution**

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table. It is not allowed to configure a VLAN to which the static MAC address belongs.

Enter a MAC address, specify a VLAN ID and select the outbound port. Then click **Add** to add a static MAC address. The MAC address entries will be updated accordingly in the MAC address table.

Static MAC Address

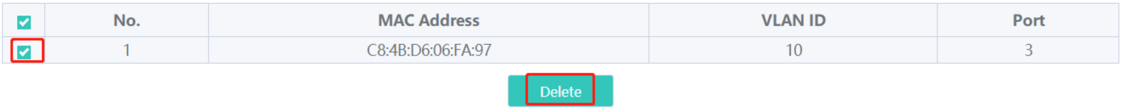


Up to 16 MAC addresses can be configured.

MAC Address	VLAN ID	Port
00:00:00:00:00:00	VLAN ID (1-4094)	Port 1 ▾

□	No.	MAC Address	VLAN ID	Port
□	1	C8:4B:D6:06:FA:97	10	3

If you want to delete a static MAC address, select the MAC address entry you want to delete in the table and click **Delete**.



☑	No.	MAC Address	VLAN ID	Port
☑	1	C8:4B:D6:06:FA:97	10	3

3.2 VLAN Settings

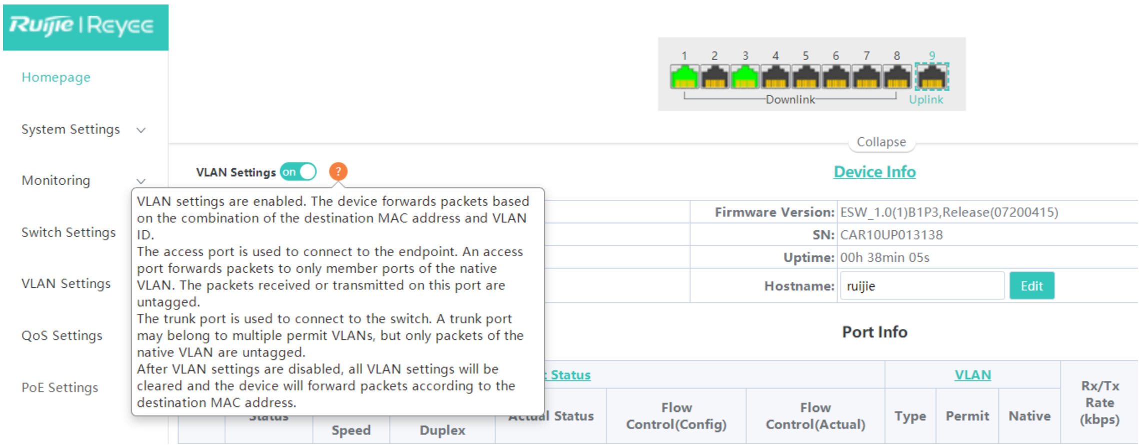
3.2.1 Global VLAN Settings

Choose **Homepage** > **Device Info**.

This page displays the status of VLAN settings. Toggle the **on-off** switch to enable or disable VLAN settings.

When VLAN is disabled, the device operates like an un-managed switch. The device forwards packets according to the destination MAC address, and the VLAN information of the forwarding packets remains unchanged during the forwarding process.

When VLAN is enabled, the device operates like a managed switch. The device forwards packets according to the destination MAC address and VLAN ID. Users can configure the port mode (access or trunk) based on whether a VLAN tag is carried in packets. Besides, all device ports will be initialized to access ports.



VLAN settings are enabled. The device forwards packets based on the combination of the destination MAC address and VLAN ID.
The access port is used to connect to the endpoint. An access port forwards packets to only member ports of the native VLAN. The packets received or transmitted on this port are untagged.
The trunk port is used to connect to the switch. A trunk port may belong to multiple permit VLANs, but only packets of the native VLAN are untagged.
After VLAN settings are disabled, all VLAN settings will be cleared and the device will forward packets according to the destination MAC address.

Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)
SN:	CAR10UP013138
Uptime:	00h 38min 05s
Hostname:	ruijie Edit

3.2.2 Static VLANs Settings

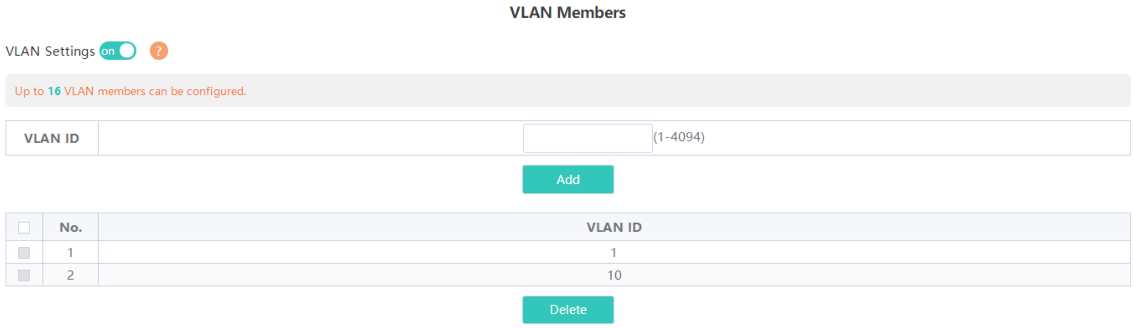
Caution

Static VLANs can be created only when the global VLAN settings feature is enabled. For details, see Chapter 3.2.1.

Choose **VLAN Settings** > **VLAN Members**.

Enter VLAN ID and click **Add** to create a static VLAN.

The VLAN table contains the existing VLANs. Select the VLANs and click **Delete**, and the corresponding VLANs will be deleted. VLAN 1 cannot be deleted.



Up to 16 VLAN members can be configured.

VLAN ID (1-4094)

□	No.	VLAN ID
□	1	1
□	2	10

Note

- The VLAN ID ranges from 1 to 4094. VLAN 1 is the default VLAN.
- The default VLAN (VLAN 1), Management VLAN, Native VLAN, Permit VLAN, and Access VLAN cannot be deleted.

3.2.3 Port VLAN Settubgs

Caution

Users can configure port VLAN only when the global VLAN settings feature is enabled. For details, see Chapter 3.2.1.

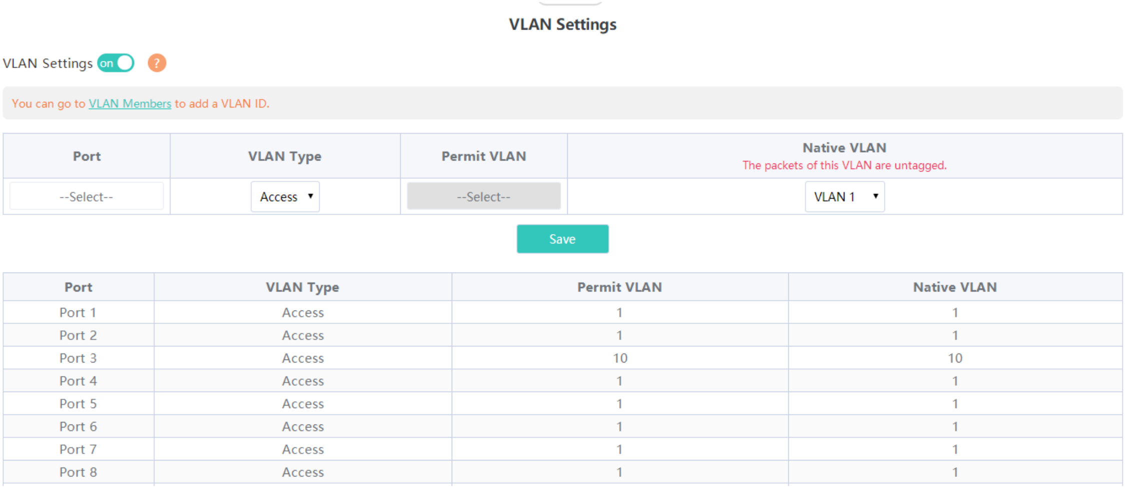
Choose **VLAN Settings** > **VLAN Settings**.

Configure the port mode and VLAN members of a port, and you will know the allowed VLANs of the port and whether the packets forwarded by the port carry tags.

Note

You are advised to create VLAN members (refer to Chapter 3.2.2) before configuring the port based on VLANs. Click **VLAN Members** to access **VLAN Members** page where you can add VLAN members.

Select the port you want to configure and the port mode. If you select the access mode, select **Access VLAN** for the port and click **Save**. If you select the trunk mode, select **Native VLAN** for the port and enter the VLAN ID range allowed by the port and click **Save**.



VLAN Settings

VLAN Settings on ?

You can go to VLAN Members to add a VLAN ID.

Port	VLAN Type	Permit VLAN	Native VLAN The packets of this VLAN are untagged.
--Select--	Access ▾	--Select--	VLAN 1 ▾

Save

Port	VLAN Type	Permit VLAN	Native VLAN
Port 1	Access	1	1
Port 2	Access	1	1
Port 3	Access	10	10
Port 4	Access	1	1
Port 5	Access	1	1
Port 6	Access	1	1
Port 7	Access	1	1
Port 8	Access	1	1

Table 3-1 Port Modes

Port Mode	Description

Access	One access port can belong to only one VLAN and allow frames from this VLAN only to pass through. This VLAN is called an access VLAN. The frames from the access port do not carry VLAN tag. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame. Access port is connected to the endpoints.
Trunk	One trunk port supports one Native VLAN and several Permit VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while Permit VLAN frames forwarded by the trunk port carry tags. Trunk port is connected to switches. Users can set the Permit VLAN range to limit VLAN frames that can be forwarded. Make sure the trunk ports at the two ends of the link are configured with the same Native VLAN.

Note

Improper configuration of VLANs on a port (especially uplink port) may cause failure to log in to the web management system. Exercise caution when configuring VLANs.

4 Security

4.1 DHCP Snooping

4.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server.

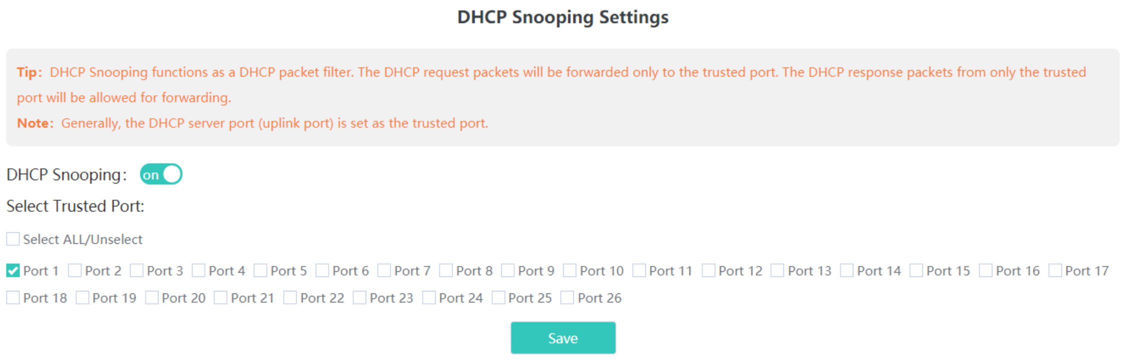
4.1.2 Configuration Steps

Choose **Switch Settings** > **DHCP Snooping Settings**.

Toggle the switch to **On** to enable DHCP snooping, select the trusted ports, and then click **Save**. When DHCP snooping is enabled, request packets from DHCP clients are forwarded only to the trusted ports. For response packets from DHCP servers, only those from the trusted ports are forwarded.

Note

The uplink port connected to the DHCP server is configured as the trusted port generally.



DHCP Snooping Settings

Tip: DHCP Snooping functions as a DHCP packet filter. The DHCP request packets will be forwarded only to the trusted port. The DHCP response packets from only the trusted port will be allowed for forwarding.

Note: Generally, the DHCP server port (uplink port) is set as the trusted port.

DHCP Snooping: on

Select Trusted Port:

□ Select ALL/Unselect

☑ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5 □ Port 6 □ Port 7 □ Port 8 □ Port 9 □ Port 10 □ Port 11 □ Port 12 □ Port 13 □ Port 14 □ Port 15 □ Port 16 □ Port 17

□ Port 18 □ Port 19 □ Port 20 □ Port 21 □ Port 22 □ Port 23 □ Port 24 □ Port 25 □ Port 26

4.2 Storm Control

4.2.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

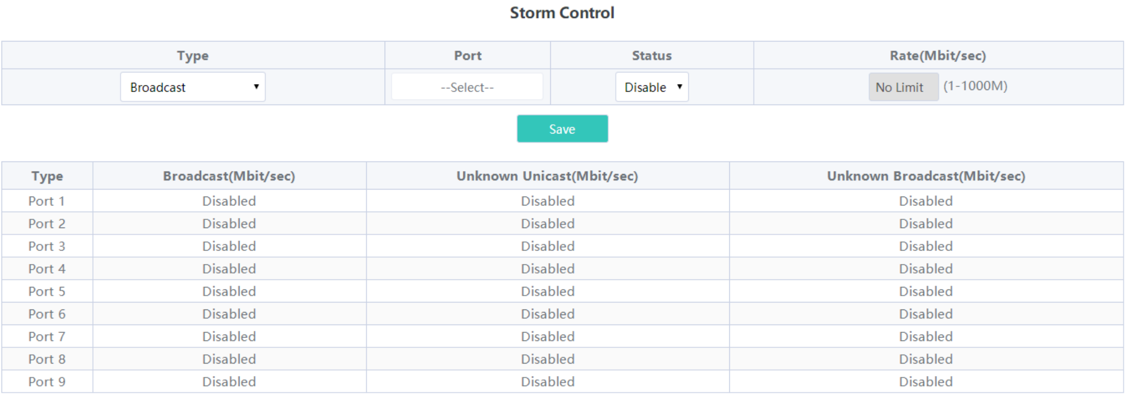
Users can perform storm control separately for the broadcast, unknown multicast, and unknown unicast data flows. When the rate of broadcast, unknown multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

4.2.2 Configuration Steps

Choose **QoS Settings** > **Storm Control**.

Select the storm control type, port, status, and enter the rate limit, and then click **Save**.

The storm control type and corresponding rate are displayed in the table right below the **Save** button. When storm control is disabled, the rate of broadcast, unknown multicast, and unknown unicast data flows is not limited. The corresponding status is displayed **Disabled**. When storm control is enabled, the corresponding rate limits will be displayed.



Storm Control

Type	Port	Status	Rate(Mbit/sec)
Broadcast ▾	--Select--	Disable ▾	No Limit (1-1000M)

Type	Broadcast(Mbit/sec)	Unknown Unicast(Mbit/sec)	Unknown Broadcast(Mbit/sec)
Port 1	Disabled	Disabled	Disabled
Port 2	Disabled	Disabled	Disabled
Port 3	Disabled	Disabled	Disabled
Port 4	Disabled	Disabled	Disabled
Port 5	Disabled	Disabled	Disabled
Port 6	Disabled	Disabled	Disabled
Port 7	Disabled	Disabled	Disabled
Port 8	Disabled	Disabled	Disabled
Port 9	Disabled	Disabled	Disabled

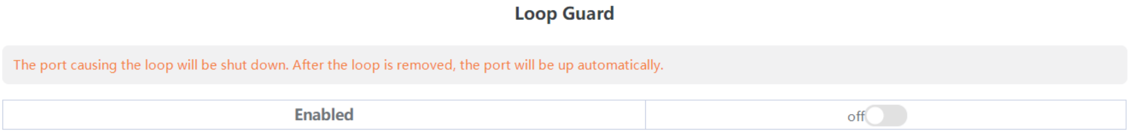
Note

- The rate limit for the ports of RG-ES220GC-P, RG-ES228GC-P switches ranges from 1Mbps to 1000Mbps.

4.3 Loop Guard

Choose **Monitoring** > **Loop Guard**.

When loop guard feature is enabled, the port causing the loop will be shut down automatically. After the loop is removed, the port will be up automatically. Loop guard function is disabled by default.



Loop Guard

The port causing the loop will be shut down. After the loop is removed, the port will be up automatically.

Enabled	off

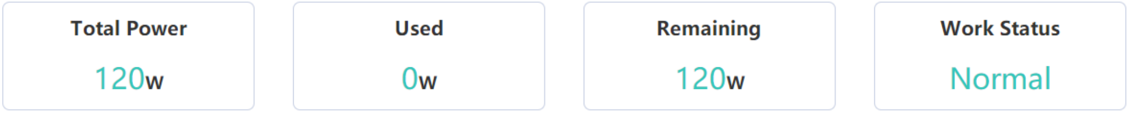
5 PoE Settings

Choose **PoE Settings**.

The device supports PoE power supply. Users can view and configure the current power status.

Device status: The total power, used power, remaining power, and current work status of the PoE system are displayed.

PoE Info

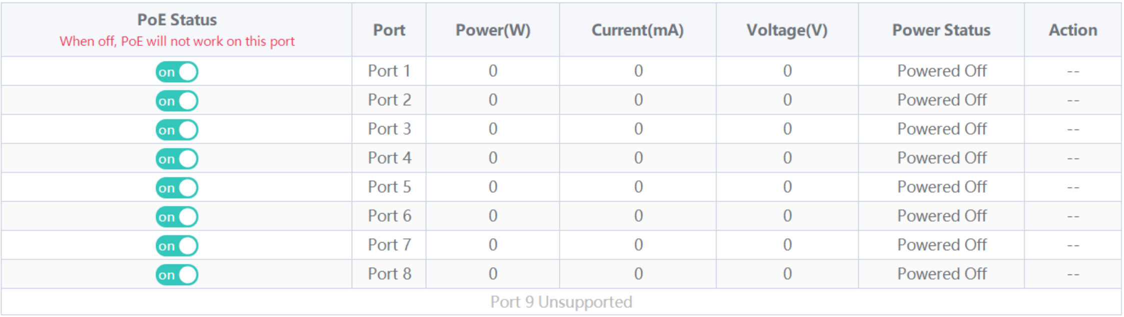


Total Power	Used	Remaining	Work Status
120w	0w	120w	Normal

Port status: The voltage, current, output power, and current power status of the device ports are displayed. Users can enable or disable PoE function through the **on-off** toggle switch. When PoE is disabled, the port will not supply power to external devices.

If a PD device fails, please power on the port connected to the PD device again to reboot it.

PoE Settings



PoE Status When off, PoE will not work on this port	Port	Power(W)	Current(mA)	Voltage(V)	Power Status	Action
on	Port 1	0	0	0	Powered Off	--
on	Port 2	0	0	0	Powered Off	--
on	Port 3	0	0	0	Powered Off	--
on	Port 4	0	0	0	Powered Off	--
on	Port 5	0	0	0	Powered Off	--
on	Port 6	0	0	0	Powered Off	--
on	Port 7	0	0	0	Powered Off	--
on	Port 8	0	0	0	Powered Off	--
Port 9 Unsupported						

Note

The fiber ports of RG-ES220GC-P, RG-ES228GC-P switches do not support the PoE function.

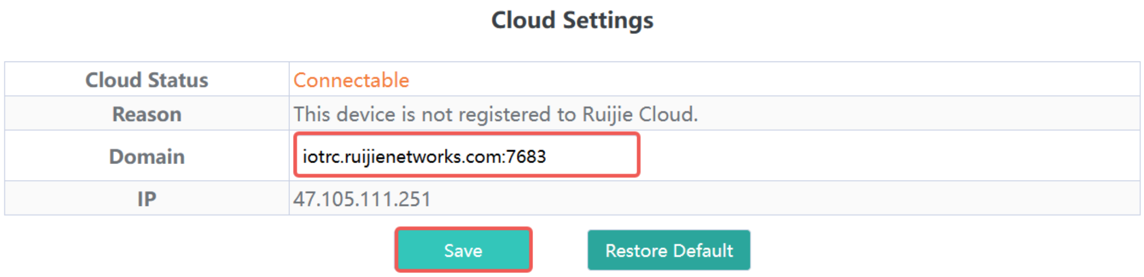
6 Diagnostics

6.1 Cloud Settings

Choose **Diagnostics** > **Cloud Settings**.

On Ruijie Cloud, you can check the status of your device, including its cloud connectivity status, reason for failure to connect, and the domain name and IP address of the cloud server.

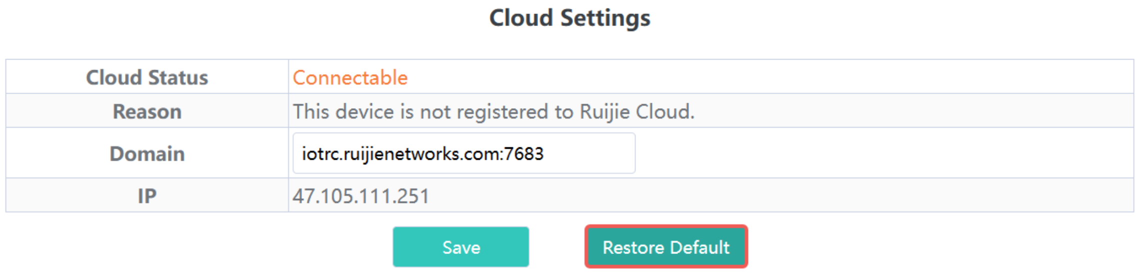
To change the domain name of the device, enter the new domain name in the **Domain** field, and then click **Save**.



Cloud Settings

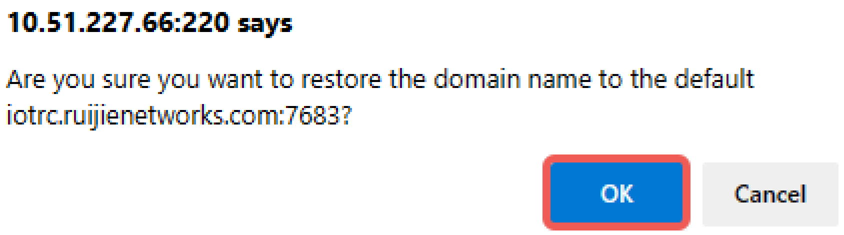
Cloud Status	Connectable
Reason	This device is not registered to Ruijie Cloud.
Domain	iotrc.ruijienetworks.com:7683
IP	47.105.111.251

To restore the default domain name, click **Restore Default**, and then click **OK** on the pop-up window.



Cloud Settings

Cloud Status	Connectable
Reason	This device is not registered to Ruijie Cloud.
Domain	iotrc.ruijienetworks.com:7683
IP	47.105.111.251



10.51.227.66:220 says

Are you sure you want to restore the domain name to the default iotrc.ruijienetworks.com:7683?

Table 6-1 Cloud Settings Parameters

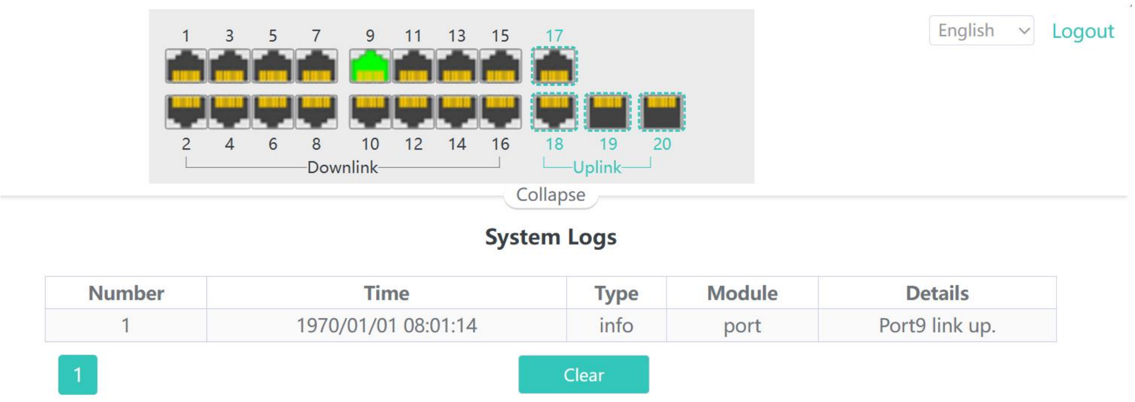
Parameter	Description
Cloud Status	Indicates the connectivity status of the device on the cloud, including Connected, Unconnected and Connectable.

Reason	Indicates the reason for connection failure. Reasons for different cloud statuses: ● Connected: No reason is displayed. ● Unconnected: o No Internet connection or DNS resolution failure. o This device failed to connect to Ruijie Cloud. ● Connectable: This device is not registered to Ruijie Cloud.
Domain	Domain name of the cloud server ⚠ **Caution** ● The coap:// prefix is not required in the domain name field as it is added by default. ● After the domain name is changed, the page is refreshed after 5 seconds by default.
IP	IP address of the cloud server resolved based on the cloud address.

6.2 System Logs

Choose **Diagnostics** > **System Logs**.

System logs record device operations, operation time, and operation modules. System logs are used by administrators to monitor the running status of the device, analyze network status, and locate faults.



System Logs

Number	Time	Type	Module	Details
1	1970/01/01 08:01:14	info	port	Port9 link up.

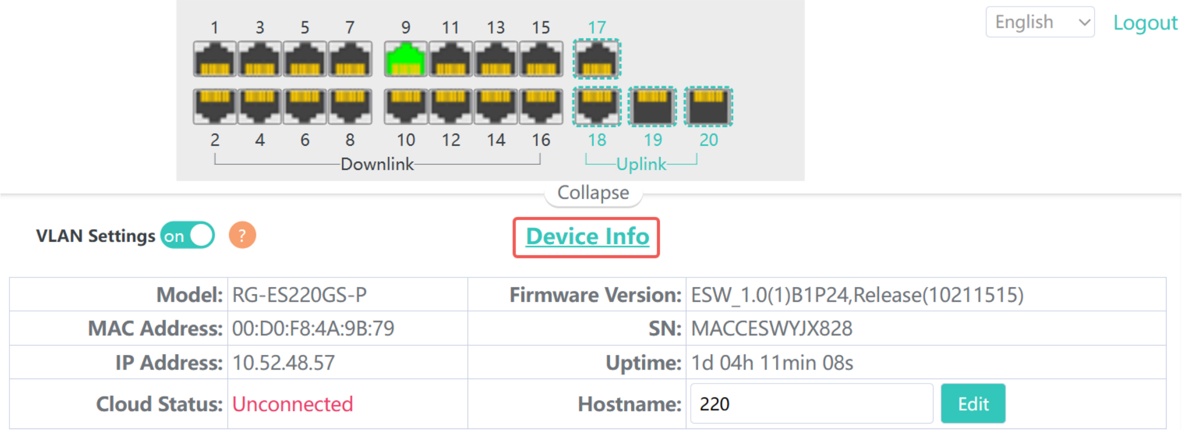
7 System Settings

7.1 Managing Device Information

7.1.1 Viewing Device Information

Choose **Homepage** > **Device Info**.

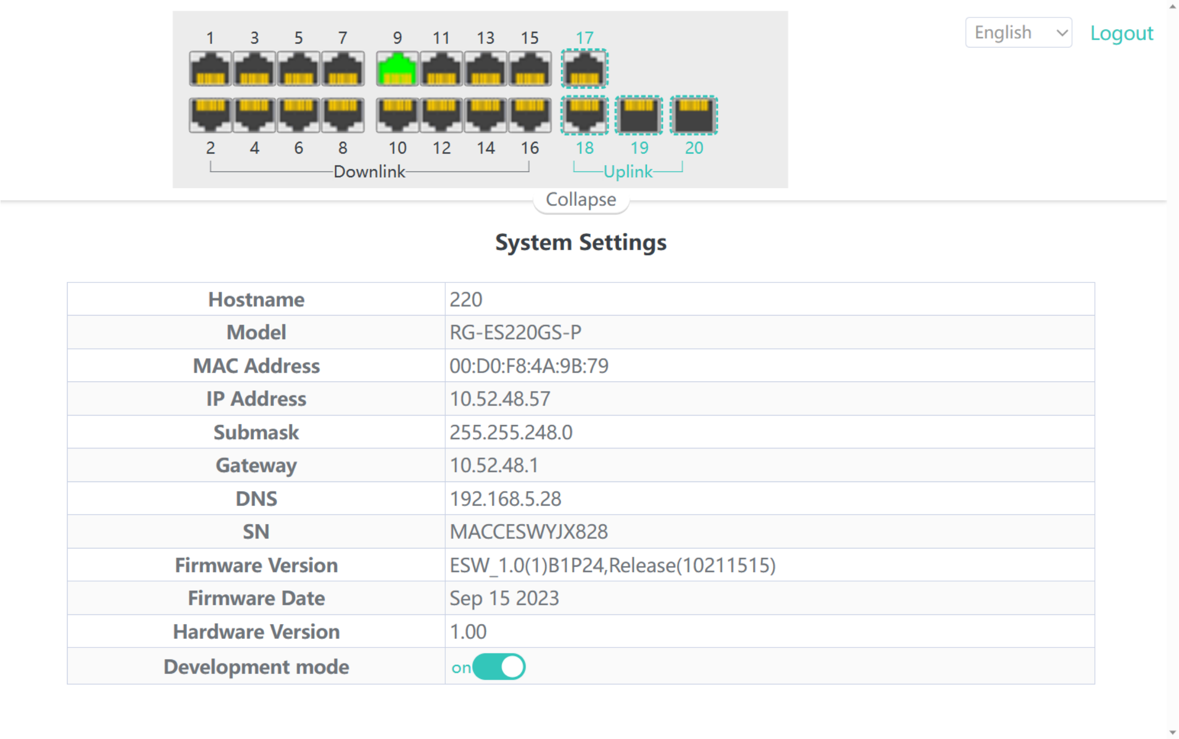
The device information is displayed on the homepage, including hostname, device model, serial number, firmware version, IP address, MAC address, cloud status, and uptime. Click **Device Info** to access the **Device Info** page (**System Settings** > **Device Info**) to view more detailed information.



VLAN Settings on ?

Device Info

Model:	RG-ES220GS-P	**Firmware Version:**	ESW_1.0(1)B1P24,Release(10211515)
MAC Address:	00:D0:F8:4A:9B:79	**SN:**	MACCESWYJX828
IP Address:	10.52.48.57	**Uptime:**	1d 04h 11min 08s
Cloud Status:	Unconnected	**Hostname:**	220 Edit



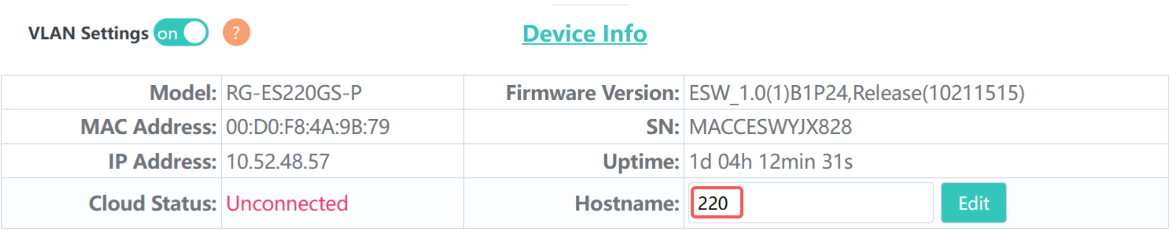
System Settings

Hostname	220
Model	RG-ES220GS-P
MAC Address	00:D0:F8:4A:9B:79
IP Address	10.52.48.57
Submask	255.255.248.0
Gateway	10.52.48.1
DNS	192.168.5.28
SN	MACCESWYJX828
Firmware Version	ESW_1.0(1)B1P24,Release(10211515)
Firmware Date	Sep 15 2023
Hardware Version	1.00
Development mode	on

7.1.2 Editing the Hostname

Choose **Homepage** > **Device Info**.

Enter the hostname and click **Edit** to edit the hostname in order to distinguish different devices.



VLAN Settings on ?

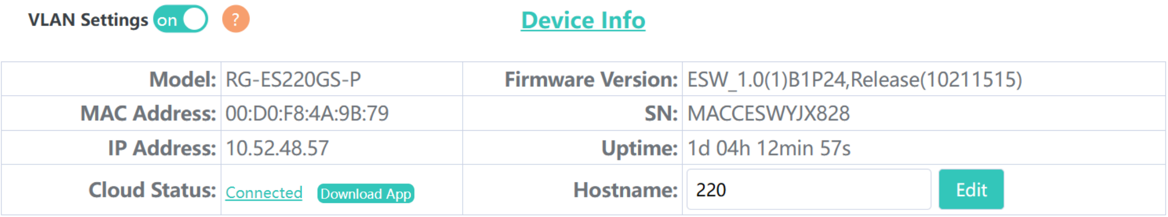
Device Info

Model:	RG-ES220GS-P	Firmware Version:	ESW_1.0(1)B1P24,Release(10211515)
MAC Address:	00:D0:F8:4A:9B:79	SN:	MACCESWYJX828
IP Address:	10.52.48.57	Uptime:	1d 04h 12min 31s
Cloud Status:	Unconnected	Hostname:	220 Edit

7.1.3 Cloud Management

Choose **Homepage** > **Device Info**.

Cloud status displays whether the device is connected to the cloud. After the device is bound to a cloud management account, the Cloud Status will display **Connected**, and users can manage the device remotely through Ruijie Cloud webpage or APP. Click **Connected** to access the homepage of Ruijie Cloud (https://cloud-as.ruijienetworks.com). Click **Download APP** to download Ruijie Cloud APP.



VLAN Settings on ?

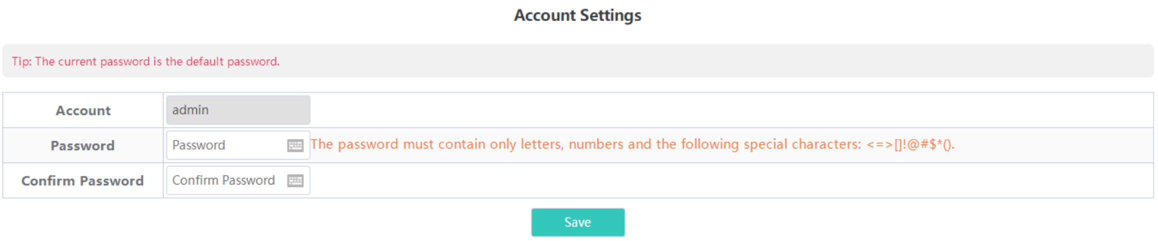
Device Info

Model:	RG-ES220GS-P	Firmware Version:	ESW_1.0(1)B1P24,Release(10211515)
MAC Address:	00:D0:F8:4A:9B:79	SN:	MACCESWYJX828
IP Address:	10.52.48.57	Uptime:	1d 04h 12min 57s
Cloud Status:	Connected Download App	Hostname:	220 Edit

7.2 Password Settings

When the device password is the default password, users will be prompted to reset the password when they log into the Eweb management system. Click **Yes** to access the **Account Settings** page (or choose **System Settings** > **Account Settings** to access the page).

Set a new password according to the tip, and then click **Save** to save the configuration.



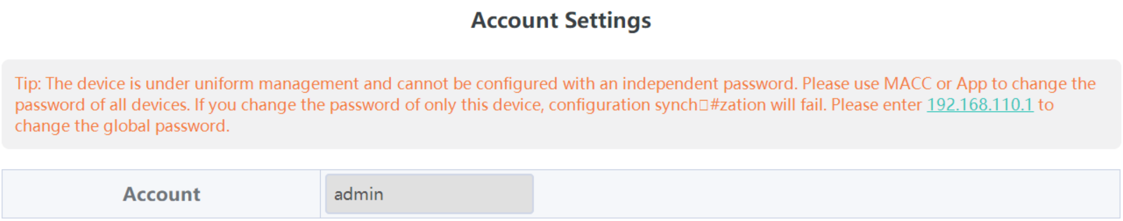
Account Settings

Tip: The current password is the default password.

Account	admin
Password	Password The password must contain only letters, numbers and the following special characters: <=>[]!@#$*().
Confirm Password	Confirm Password

Save

If the device is under uniform management, it cannot be configured with an independent password. Users need to follow the tip to log in to the master device for global password configuration.



Account Settings

Tip: The device is under uniform management and cannot be configured with an independent password. Please use MACC or App to change the password of all devices. If you change the password of only this device, configuration synch□#zation will fail. Please enter 192.168.110.1 to change the global password.

Account	admin

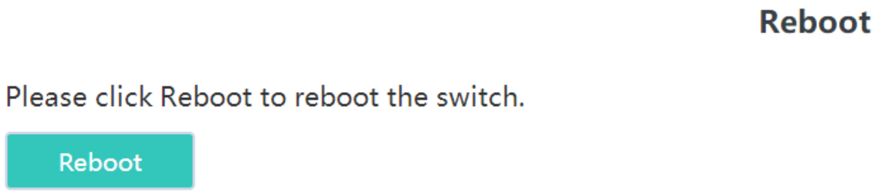
⚠ **Caution**

- Upon your initial login to the eWeb management system, you must set the device management password first before you configuring other features.
- Please remember the device management password (default username/password: admin/admin). You may need to log in again after changing the password.
- If the device has been under uniform management, please use MACC or APP to change the network-wide password. Changing the password of this device will cause failure to synchronize network-wide settings to this device.

7.3 Device Reboot

Choose **System Settings** > **Reboot**.

Click **Reboot** to reboot the switch.



Reboot

Please click Reboot to reboot the switch.

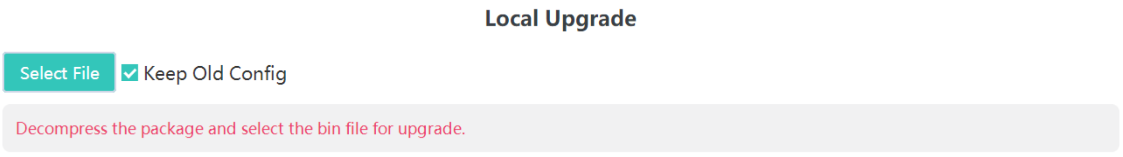
7.4 System Upgrade

7.4.1 Local Upgrade

Choose **System Settings** > **Upgrade**.

Click **Select File** to select the upgrade package from the local files (the upgrade package is a bin file. If it is a tar.gz file, users need to decompress the package and select the bin file for upgrade).

Keep Old Config is selected by default. That means the current configuration will be saved after device upgrade. If there is a huge difference between the current version and the upgrade version, you are advised not to select **Keep Old Config**.



Local Upgrade

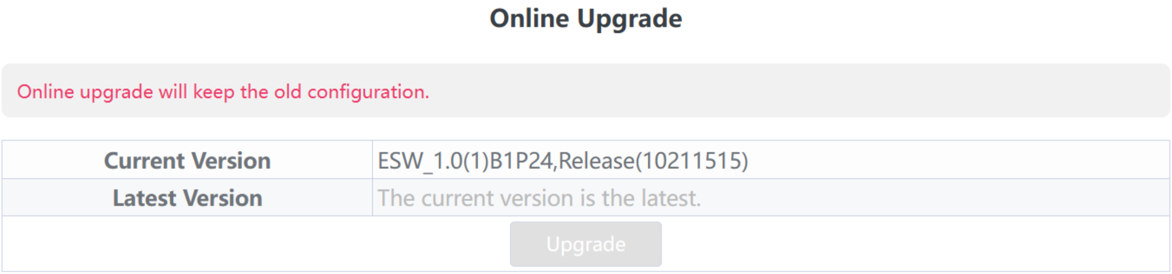
☑ Keep Old Config

Decompress the package and select the bin file for upgrade.

7.4.2 Online Upgrade

Choose **System Settings** > **Upgrade**.

When there is a new version in the cloud, the version number of the latest version will be displayed on this page, and the **Upgrade** button will become available. The device will download the installation package of the recommended version from the cloud and it will be updated to the latest version. Online upgrade will keep the old configuration by default.



Online Upgrade

Online upgrade will keep the old configuration.

Current Version	ESW_1.0(1)B1P24,Release(10211515)
Latest Version	The current version is the latest.

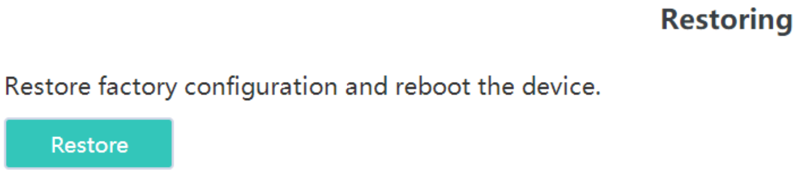
Note

The time that online upgrade takes depends on the current network speed. It may take some time. Please be patient.

7.5 Restoring Factory Configuration

Choose **System Settings** > **Restore Default**.

Click **Restore** to restore factory configuration and reboot the device.



Restoring

Restore factory configuration and reboot the device.

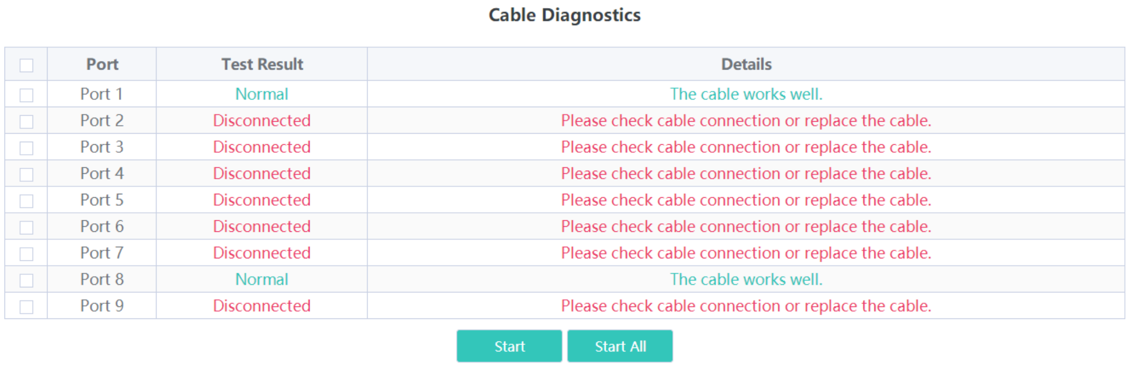
8 Monitoring

8.1 Cable Diagnostics

Choose **Monitoring** > **Cable Diagnostics**.

Cable diagnostics allows users to check the status of Ethernet cables. For example, users can check whether the cables are short-circuited or disconnected.

Select the ports you want to detect, and then click **Start** to start cable diagnostics. The test result will be displayed accordingly. Click **Start All** to perform one-click cable diagnostics on all ports.



Cable Diagnostics

□	Port	Test Result	Details
□	Port 1	Normal	The cable works well.
□	Port 2	Disconnected	Please check cable connection or replace the cable.
□	Port 3	Disconnected	Please check cable connection or replace the cable.
□	Port 4	Disconnected	Please check cable connection or replace the cable.
□	Port 5	Disconnected	Please check cable connection or replace the cable.
□	Port 6	Disconnected	Please check cable connection or replace the cable.
□	Port 7	Disconnected	Please check cable connection or replace the cable.
□	Port 8	Normal	The cable works well.
□	Port 9	Disconnected	Please check cable connection or replace the cable.

⚠ **Caution**

If you select an uplink port for diagnostics, the network may be intermittenly disconnected. Exercise caution when performing this operation.

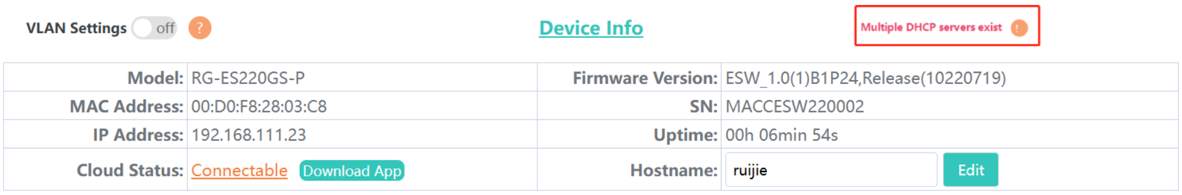
8.2 Multi-DHCP Alarming

⚠ **Caution**

Multi-DHCP alarming will fail when the device IP address is not obtained dynamically. For relevant IP address configuration, see Chapter 2.6.

Choose **Homepage**.

When there are multiple DHCP servers in a LAN, the system will send a conflicting alarm. An alarming message will be displayed in the **Device Info** column.



Multiple DHCP servers exist !

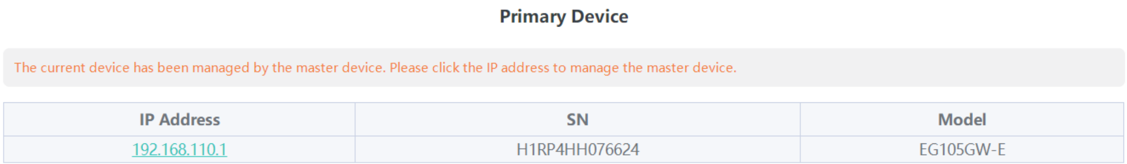
Model:	RG-ES220GS-P	Firmware Version:	ESW_1.0(1)B1P24,Release(10220719)
MAC Address:	00:D0:F8:28:03:C8	SN:	MACCESW220002
IP Address:	192.168.111.23	Uptime:	00h 06min 54s
Cloud Status:	Connectable Download App	Hostname:	ruijie Edit

Move the cursor to ? to view the alarm details, including the VLAN where the conflicts occur, port, IP address of DHCP server, and MAC address.

8.3 Viewing Switch Information

Choose **Monitoring** > **Switches**.

If the switch is under uniform management, some features cannot be configured independently (such as password settings). To facilitate configuration, information of the master device in the VLAN will be displayed in this page. Click the **IP Address** of the master device to access **Master Device** page for global configuration.



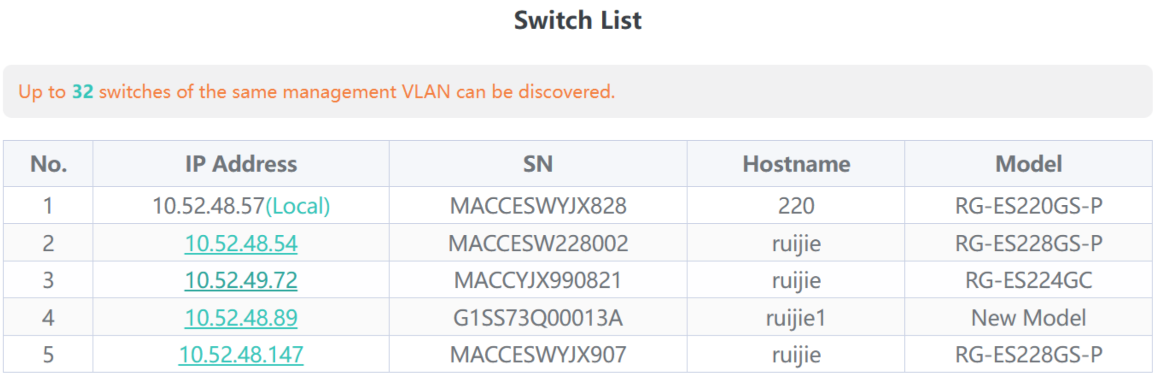
Primary Device

The current device has been managed by the master device. Please click the IP address to manage the master device.

IP Address	SN	Model
192.168.110.1	H1RP4HH076624	EG105GW-E

The device is able to automatically discover other switches in the same management VLAN. Information of these switches will be displayed in **Switch List**.

The first row of **Switch List** displays information of the current device, and the following rows display information of other devices. Click **IP Address** of a device to access the Eweb management system of the device (login required).



Switch List

Up to 32 switches of the same management VLAN can be discovered.

No.	IP Address	SN	Hostname	Model
1	10.52.48.57(Local)	MACCESWYJX828	220	RG-ES220GS-P
2	10.52.48.54	MACCESW228002	ruijie	RG-ES228GS-P
3	10.52.49.72	MACCYJX990821	ruijie	RG-ES224GC
4	10.52.48.89	G1SS73Q00013A	ruijie1	New Model
5	10.52.48.147	MACCESWYJX907	ruijie	RG-ES228GS-P

Note

The number of switches that can be discovered varies with product modes:

- RG-ES220GC-P, RG-ES228GC-P can discover 32 switches.

9 FAQs

Q1: I failed to log into the web management system. What can I do?

(1) Verify that the Ethernet cable is properly connected to the LAN port of the device and the LED indicator blinks or is steady on.

(2) Before accessing the web management system, you are advised to configure the PC with a static IP address in the same network segment as the device IP address (default device IP address: 10.44.77.200 and subnet mask: 255.255.255.0). For example, set the IP address of the PC to 10.44.77.100 and the subnet mask to 255.255.255.0.

(3) Run the **ping** command to test the connectivity between the PC and the device.

(4) If the login failure persists, restore the device to factory settings.

Q2: What can I do if I forget my username and password? How to restore the factory settings?

(1) Log in with the default username and password (default username/password: admin/admin).

(2) If you fail to log in with the default password, restore the factory settings. To restore the factory settings, please power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. After device restart, you can log into the web management system by accessing the default management IP address (10.44.77.200).